Introduction

This document describes how to set up FreeRADIUS server in order to authenticate Windows users transparently against Active Directory.

Principles

FreeRADIUS offers authentication via port based access control. A user can connect to the network only if its credentials have been validated by the authentication server. User credentials are verified by using special authentication protocols which belong to the 802.1X standard.

Prerequisites

The following components are required to install the access control solution:

- A Linux 5.8 or higher version
- FreeRADIUS 2.0.x
- Samba 3.0.x
- Openssl
- Windows AD

Set up the Linux server

Linux must be configured to join a Windows domain. This is done by using the Samba file server which offers several interesting tools. The goal is not to create a Samba file server but only to use some tools which come with this server.

Samba server contains among others the following components:

- Winbind, a daemon which permits connectivity to Windows –NT environment.
- ntlm_auth, a tool which uses winbind for evaluating NTLM (NT Lan Manager) requests. This tool allows verifying user credentials on the domain controller and returns either a success or an error message.

1. Please have a look at your Linux box and check if Samba is already installed

```
#rpm –qa | grep samba
```

If you Find the file smb.conf

```
# find / -name smb.conf
```

2. And open it with your preferred editor.

The file must contain the following lines:

In the [global] section

```
# workgroup = NT-Domain-Name or Workgroup-Name
  workgroup = XYZDOM  //the name of your domain

  security = ads


======== Share Definitions ========

 ...
 winbind use default domain = no
 password server = XYZSRV.XYZ-COMPANY.COM //your AD-server
 realm = XYZ-COMPANY.COM      //your realm
```

Verify the following lines in the [homes] section

```
comment = Home Directories
browseable = no
writable = yes
```

3. Next, find the file `krb5.conf`. Normally it should be found in `/etc/krb5.conf`.

   Edit this file with the following information: (Watch out for case sensitivity)

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false

[realms]
 EXAMPLE.COM = {
  kdc = kerberos.example.com:88
  admin_server = kerberos.example.com:749
  default_domain = example.com
 }

 XYZ-COMPANY.COM = {
  kdc = XYZSRV.XYZ-COMPANY.COM
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM

[kdc]
  profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
  debug = false
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
 }
```

4. Edit the file `/etc/nsswitch.conf` and add *winbind* at the end of each line shown below

```
passwd:     files winbind
shadow:     files winbind
group:      files winbind
protocols:  files winbind

services:   files winbind

netgroup:   files winbind

automount:  files winbind
```

5. Restart the machine.

6. After restart,Verify if the Samba service is running by typing

```
#ps –ef | grep nmbd
#ps –ef | grep smbd
```

if nothing output comes then you have to start the service by using

```
#service smb start
#service nmb start
```

7. Execute the following command line (you must be connected as root)

```
#net join –U Administrator
```

Administrator is the name of the domain controller admin. Enter your password when prompted. If everything works fine, the Linux server has been registered to the Windows domain.

8. Verify now if the winbindd daemon is running

```
#ps –ef | grep winbindd
```

9. Try next if you can authenticate a user from the domain

```
#wbinfo –a user%password
```

The output should be something like the following

```
wbinfo –a example_user%mypassword
plaintext password authentication failed
error code was NT_STATUS_NO_SUCH_USER (0xc0000064)
error message was: No such user
Could not authenticate user example_user%mypassword with plaintext
password
```

10. Let’s try to authenticate with NTLM, which is necessary for using FREERADIUS with Active Directory.

    Type the following line

    ```
    #ntlm_auth --request-nt-key --domain=<your domain> --username=<your username>
    ```

    The command line returns

    ```
    NT_STATUS_OK : Success (0x0)
    ```

11. Open up /etc/raddb/clients.conf through command

    ```
    #vim /etc/raddb/clients.conf
    ```

    Enter the clients detail.which will be interact with your radius server.

    Example:

    ```
    client IP {
        secret         = YOUR SECRET HERE
        shortname              = yourVPN
        nastype                = other
    }
    ```

12. Open up /etc/raddb/proxy.conf

    ```
    #vim /etc/raddb/proxy.conf
    ```

    Enter the National and your domain detail.

    Example:

    ```
    realm Default {
        authhost               = National IP
        secret         = YOUR SECRET HERE
        shortname              = yourVPN
        nostrip
    }

    realm xyz.in {
        Authhost               = LOCAL
    }
    ```

13. Open /etc/raddb/eap.conf

    Replace the line `default_eap_type = md5` with `default_eap_type = peap`

    And in ttls section and peap section,change

```
default_eap_type = mschapv2
copy_request_to_tunnel = yes
use_tunneled_reply = yes
```

14. Now check to see if Radius is working ok or not:

    use

```
#service radiusd restart
```

If your radius service start become fail,then you can check the error by using

```
#radiusd –X
```

It will tell the error

If no error occur
Congratulation!!!

You have successfully configured radius server against active directory authentication .